2016年度セキュリティ委員会成果報告

一般社団法人 日本画像医療システム工業会（JIRA)
医用画像システム部会　セキュリティ委員会　五十嵐　隆史

はじめに

- 16年7月に委員長、副委員長人事を変更。
  委員長：五十嵐
  副委員長：西田、野津、梶山

目次

2016年度の主な活動

- ISO/TC215 WG4(セキュリティ&プライバシ)で検討されている国際標準への対応を行った。
- 厚生労働省「※医療情報システムの安全管理に関するガイドライン」に対して、ベンダの立場で取り組みを行った。　※以下、安全管理GLと表記
- 医療機器におけるサイバーセキュリティへの対応を行った。
- リモートサービスセキュリティ・ガイドラインの改訂および「製造業者による医療情報セキュリティ開示書」ガイド(MDS)の改訂、普及活動を行った。
- IoTセキュリティガイドライン、改正個人情報保護法に関する情報共有を行った。

ISO/TC215 WG4

- 年2回開催されている会議へエキスパートを派遣
  - 2016年5月　アムステルダム(NL)　2名
  - 2016年11月　リレハンメル(NO)　1名
  - 2017年4月(予定)　杭州(CN)　2名

- 規格検討への積極的な取り組み
  - 新規作業項目へエキスパートとして登録
  - ドラフトの内容検討、JIRAとしての意見集約
  - JIRAの主張のドラフトへの反映

- 日本からの規格提案
  - リモートサービスセキュリティWG(RSS-WG)で作成したガイドラインがベースとなっているTR11633の改定提案(TS化)

●検討中の主な国際標準

1）ISO/PWI TR 21332 Health informatics Cloud computing security and privacy requirements for health information

ブラジルから提案されている PWI（Preliminary Work Item）。

クラウド・コンピューティングにおけるセキュリティとプライバシー要件

2）ISO/IS PWI 20429 Priciples and guidelines for protection of personal health information

個人健康情報保護の原則とガイドライン

3）ISO/IS 17090 PKI-Digital signatures for healthcare documents

日本提案のPKIを利用したヘルスケア文書への電子署

4）ISO/TS 11633 Part1

RSS-WGにおいて規格作成を実施。後述。

5）ISO 13606- Part 4 Electronic health record communication -- Part 4: Security

診療記録の通信に関するWG1とのジョイント規格

6）ISO 27789 Audit trails for electronic health records

監査証跡に関する規格

ISO/TC215 WG4

- その他関連する国際規格

1) ISO/IEC81001-1 Health software and health IT system safety, effectiveness and security – Foundational principles, concepts, and terms

2) DICOM WG14(Security)関係

3) RSP (Referenced Standard Portfolio) bundle Clinical Imaging

4) IEC 80001シリーズ

5) IEC 62304 Ed.2

6) IEC 82304-1

RSS-WG

- リモートサービスセキュリティガイドライン Ver.3.0への改訂作業
  - 医療機関内の情報機器・システムを遠隔保守するケースのモデル化を行い、そのモデルに対してISMS（Information Security Management System）の手法に従ったリスクマネジメントの実施例を提示
  - 最新版のISO27000シリーズに対応
  - 経産省ガイドライン改定、JIPDEC ISMSユーザガイド最新版への対応
  - 附属にリスクアセスメント例を記載
  - ✓ JESRA TR－0034*B－2016として16年8月に改訂版発行

RSS-WG

- ISO/TS11633-1改定作業
  - JESRAの「リモートサービスセキュリティガイドライン」とほぼ同じ内容
  - アムステルダム会議(16年5月)においてFORM4がFIX
  - リレハンメル会議(16年11月)でコメント処理を実施
  - 杭州会議(17年4月)に向け1stWDを作成中

✓1stWDを3月1日までに提出予定

✓当面はISO/TS11633対応が主活動

厚生労働省「安全管理ガイドライン」

- 厚生労働省「医療情報システムの安全管理に関するガイドライン 第5版」に対しての取り組み
  - 改定を行う作業班へ2名参加
  - 厚労省からのインタビューを受ける
  - 個人情報保護法に関しては再検討が必要となり対象から外れた。そのため、それ以外の内容を**第4.4版**として改定作業が進められている
  - 現在パブリックコメント中
  - 以下の項目が改定される見込み

厚生労働省「安全管理ガイドライン」

●第4.4版の主な改定項目

1. 電子カルテの代行入力を時間経過で自動確定することへの言及
2. 「製造業者による情報セキュリティ開示書」ガイドVer.2.0への言及
3. モバイルデバイスへの対応
4. 標的型攻撃への対応
5. 個人情報保護法への対応　(見送り)
6. TLS1.2によるオープンネットワーク接続への言及
7. 小規模医療機関が順守すべき項目の明確化
8. 医療情報システムの対象範囲の検討
9. IoTセキュリティへの対応
10. 2要素認証の採用
11. 電子署名の採用
12. わかりやすさへの対応
13. 規格変更への対応

厚生労働省「安全管理ガイドライン」

- 広報活動
  - 第44回日本放射線技術学会秋季学術大会
    - JIRAワークショップ(16年10月)
  - JIRA　IT特区勉強会（17年02月）

- 今後の対応
  - 第4.4版に関しては正式版が公開後、MDSを通して周知を行っていく。
  - 第5版に関しては個人情報保護法への対応を含め引き続き対応を継続する。

MDS-WG

- MDSは「製造業者による医療情報セキュリティ開示書（Manufacturer Disclosure Statement for Medical Information Security）」の略称
- JAHIS-JIRA合同開示書WGにて2013年4月に作成され、現在Ver.2.0。JAHIS標準およびJESRA化
- 厚生労働省「医療情報システムの安全管理に関するガイドライン」への適合を示すチェックリストと、書き方を示したガイド
- 製造業者が医療機関に対し、医療情報機器・システムの情報セキュリティに関する情報を開示する際に使用することを目的

MDS-WG

製造業者による医療情報セキュリティ開示書　チェックリスト　第2版

製造メーカ　：XYZ 株式会社	作成日　：2016 年 1 月 26 日
製品名称　：General-PACS	バージョン　：V1.20R00

医療機関における情報セキュリティマネジメントシステムの実践（6.2）				
1　扱う情報のリストを提示してあるか？（6.2.C1）	(はい)	いいえ	対象外	備考 1
物理的安全対策（6.4）				
2　窃視防止の機能があるか？（6.4.C5）	はい	(いいえ)	対象外	備考 2
技術的安全対策（6.5）				
3　不正入力防止の機能があるか？（6.5.C3）	(はい)	いいえ	対象外	備考 3
4　アクセス管理の機能があるか？（6.5.C1、6.5.C5）	(はい)	いいえ	対象外	備考
4．1　アクセス管理の認証方式は？（6.5.C1）				
・パスワード認証	(はい)	いいえ	対象外	備考
・生体認証	(はい)	いいえ	対象外	備考 4
・物理媒体認証	はい	(いいえ)	対象外	備考
・二要素認証	はい	(いいえ)	対象外	備考
・その他（具体的な方法を備考に記入してください）	はい	(いいえ)	対象外	備考
4．1．1　パスワードを利用者認識手段として利用している場合、パスワード管理は可能か？（6.5.C10-1～6.5.C10-3）	はい	(いいえ)	対象外	備考 5
4．2　アクセスログを出力する機能があるか？（6.5.C6）	(はい)	いいえ	対象外	備考
4．2．1　アクセスログを利用者が確認する機能があるか？（6.5.C6）	はい	(いいえ)	対象外	備考 6
4．2．2　アクセスログへのアクセス制限が出来るか？（6.5.C7）	(はい)	いいえ	対象外	備考
5　時刻情報の正確性を担保する仕組みがあるか？（6.5.C8）	(はい)	いいえ	対象外	備考 7
6　不正ソフトウェア対策を行っているか？（6.5.C9）	(はい)	いいえ	対象外	備考 8
7　無線 LAN を利用する場合のセキュリティ対策機能はあるか？（6.5.C.11）	はい	(いいえ)	対象外	備考 9
情報および情報機器の持ち出しについて（6.9）				
8　ソフトウェアのインストールを制限する機能があるか？（6.9.C9）	はい	(いいえ)	対象外	備考 10
9　外部入出力装置の機能を無効にすることができるか？（6.9）	はい	(いいえ)	対象外	備考 11
10　管理区域外への持ち出しの際、起動パスワード等のアクセス制限を設定できるか？（6.9.C6、6.9.C7）	はい	いいえ	(対象外)	備考
災害等の非常時の対応（6.10）				
11　非常時機能又は、非常時アカウントを持っているか？（6.10.C1）	はい	(いいえ)	対象外	備考 12
外部と個人情報を含む医療情報を交換する場合の安全管理（6.11）				
12　外部と個人情報を含む医療情報を通信する機能やリモート保守機能を有するか？（6.11.C1）	(はい)	いいえ	対象外	備考 13
12．1　なりすましの対策（認証）機能を有するか？（6.11.C3）	(はい)	いいえ	対象外	備考
12．2　データの暗号化（SSL、S/MIME、ファイル暗号化など）が可能か？（6.11.C5）	(はい)	いいえ	対象外	備考
12．3　ネットワークの経路制御・プロトコル制御に関わる機能を有しているか？（6.11.C4）	はい	(いいえ)	対象外	備考 14
12．3．1　ネットワークの経路制御・プロトコル制御に関わる機能は、安全管理ガイドラインを満たす設定が可能か？（6.11.C4）	はい	いいえ	対象外	備考
12．3．2　ネットワークの経路制御・プロトコル制御に関わる機能の適正さを証明できる文書があるか？（6.11.C4）	はい	いいえ	対象外	備考
12．4　リモートメンテナンス機能を有するか？（6.11.C7）	(はい)	いいえ	対象外	備考 13
12．4．1　リモートメンテナンスサービスに関し、不必要なリモートログインを制限する機能があるか？（6.11.C7）	(はい)	いいえ	対象外	備考
法令で定められた記名・押印を電子署名で行うことについて（6.12）				
13　記名・押印が義務付けられた文書を扱っているか？（6.12.C.(1)）	(はい)	いいえ	対象外	備考
13．1　HPKI 対応もしくは特定認定認証局が発行する証明書対応の署名機能があるか？（6.12.C.(1)）	はい	(いいえ)	対象外	備考 15
13．2　HPKI 対応もしくは特定認定認証局が発行する証明書対応の検証機能があるか？（6.12.C.(1)）	はい	(いいえ)	対象外	備考 15
13．3　日本データ通信協会認定のタイムスタンプが付与可能か？（6.12.C.(2)）	はい	(いいえ)	対象外	備考 15
13．4　日本データ通信協会認定のタイムスタンプが検証可能か？（6.12.C.(2)）	はい	(いいえ)	対象外	備考 15
13．5　保存期間中の文書の真正性を担保する仕組みがあるか？（6.12.C.(2)）	はい	(いいえ)	対象外	備考 15

MDS-WG

真正性の確保について（7.1）

１４　利用者を正しく識別し、認証を行う機能があるか？(7.1.C.(1).a-1)　(はい)　いいえ　対象外　備考＿＿

１４．１　区分管理を行っている対象情報ごとに、権限管理（アクセスコントロール）の機能があるか？(7.1.C.(1).a-2)
(はい)　いいえ　対象外　備考＿＿

１４．２　権限のある利用者以外による作成、追記、変更を防止する機能があるか？(7.1.C.(1).a-2)
(はい)　いいえ　対象外　備考＿＿

１５　システムが端末を管理することによって、権限を持たない者からのアクセスを防止する機能があるか？(7.1.C.(1).a-3)
(はい)　いいえ　対象外　備考＿＿

１６　システムは記録を確定する機能があるか？（7.1.C.(2).a-1）　(はい)　いいえ　対象外　備考＿＿

１６．１　確定情報には、作成責任者の識別情報、信頼できる時刻源を用いた作成日時が含まれているか？
(7.1.C.(2).a-1)　(はい)　いいえ　対象外　備考 16

１６．２　「記録の確定」を行うにあたり、作成責任者による内容の確認をする機能があるか？（7.1.C.(2).a-2）
(はい)　いいえ　対象外　備考＿＿

１６．３　確定された記録に対して、故意による虚偽入力、書き換え、消去及び混同を防止する機能があるか？
(7.1.C.(2).a-3)　(はい)　いいえ　対象外　備考＿＿

１７　装置が確定機能を持っていない場合、記録が作成される際に、作成責任者の識別情報、作成日時を含めて記録する機能があるか？（7.1.C.(2).b-1）　はい　いいえ　(対象外)　備考＿＿

１８　確定された診療録等が更新された場合、更新履歴を保存し、更新前後の内容を参照する機能があるか？（7.1.C.(3)-1）
はい　(いいえ)　対象外　備考 17

１８．１　同じ診療録等に対して更新が複数回行われた場合、更新の順序性を識別できる機能があるか？（7.1.C.(3)-2）
はい　いいえ　対象外　備考＿＿

１９　代行操作の承認機能があるか？（7.1.C.(4)）　はい　(いいえ)　対象外　備考＿＿

１９．１　代行操作が行われた場合、誰の代行が誰によっていつ行われたかの管理情報を、その代行操作の都度、記録する機能があるか？（7.1.C.(4)-2）　はい　いいえ　対象外　備考＿＿

１９．２　代行操作により記録された診療録等を、作成責任者による「確定操作（承認）」を行う機能があるか？(7.1.C.(4)-3)
はい　いいえ　対象外　備考＿＿

見読性の確保（7.2）

２０　目的に応じて速やかな検索結果の出力機能があるか？（7.2.C.(3)）　(はい)　いいえ　対象外　備考＿＿

２１　システム障害に備えた冗長化手段はあるか？（7.2.C.(4)）　(はい)　いいえ　対象外　備考＿＿

２１．１　冗長化の内容は？(7.2.C.(4))
・サーバの冗長化　はい　(いいえ)　対象外　備考＿＿
・ネットワークの冗長化　はい　(いいえ)　対象外　備考＿＿
・ストレージの冗長化　(はい)　いいえ　対象外　備考＿＿
・その他の手段(具体的な方法を備考欄に記入してください)　備考＿＿

２２　システム障害に備えた代替え的な見読化手段があるか？（7.2.C.(4)）　(はい)　いいえ　対象外　備考 18

保存性の確保（7.3）

２３　いわゆるコンピュータウイルスを含む不適切なソフトウェアによる情報の破壊・混同が起こらないようにするための防護機能があるか？（7.3.C.(1)-1）　(はい)　いいえ　対象外　備考 8

２４　記録媒体及び記録機器の保管及び取扱いについて、医療機関等が運用管理規程を定めるために必要な情報が、操作マニュアル等の文書として提供されているか？（7.3.C.(2)-1）　(はい)　いいえ　対象外　備考＿＿

２５　情報の保存やバックアップについて、医療機関等が運用管理規程を定めるために必要な情報が、操作マニュアル等の文書として提供されているか？（7.3.C.(2)-2）　(はい)　いいえ　対象外　備考＿＿

２６　システムが保存する情報へのアクセスについて、履歴を残す機能があるか？（7.3.C.(2)-4）　(はい)　いいえ　対象外　備考＿＿

２６．１　システムが保存する情報へのアクセスについてその履歴を管理するための機能があるか？（7.3.C.(2)-4）
はい　(いいえ)　対象外　備考 19

２７　システムが保存する情報がき損した時に、バックアップされたデータを用いて、き損前の状態に戻すための機能があるか？（7.3.C.(2)-5）　(はい)　いいえ　対象外　備考 20

２８　記録媒体が劣化する以前に情報を新たな記録媒体または記録機器に複写する機能があるか？（7.3.C.(3)-1）　(はい)　いいえ　対象外　備考＿＿

２９　システムの移行の際に診療録等のデータを標準形式が存在する項目に関しては標準形式で、標準形式が存在しない項目では変換が容易なデータ形式にて出力及び入力できる機能があるか？（7.3.C.(4)-1）　(はい)　いいえ　対象外　備考 21

診療録等をスキャナ等により電子化して保存する場合について（9.）

３０　診療録などをスキャナなどにより電子化して保存する機能があるか（9.1.C-1）（9.4.）　(はい)　いいえ　対象外　備考 22

３０．１　光学解像度、センサ等の一定の規格・基準を満たすスキャナを用いているか？（9.1.C-1）　(はい)　いいえ　対象外　備考 23

３０．２　電子署名・タイムスタンプ等を行える機能があるか？（9.1.C-2）（9.4.C-2）　はい　(いいえ)　対象外　備考 15

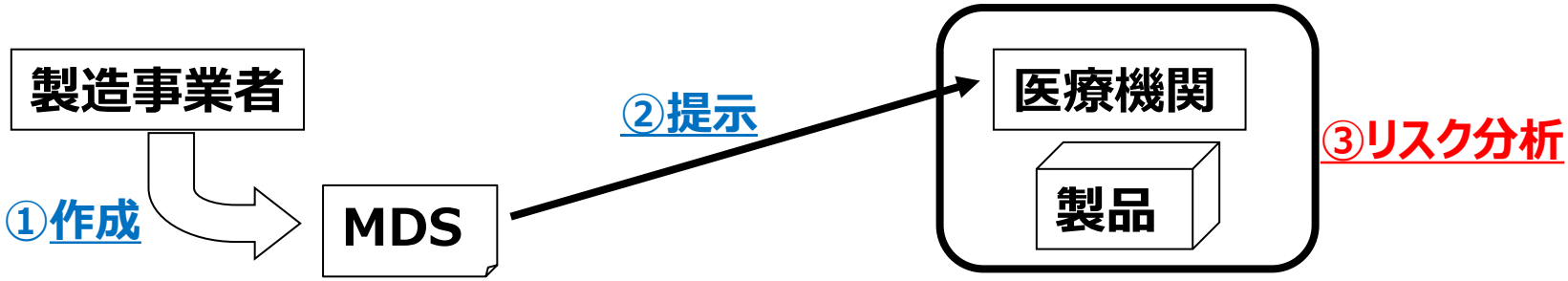
	備考記載欄
1	DICOM CONFORMANCE STATEMENT 中に情報リストの記載があります。
2	窃視される危険性の無い環境でご利用下さい。
3	離席時にはワンボタンで画面ロックする機能があります。
4	オプションの機器が必要となります。詳細は弊社担当者に問い合わせください。
5	パスワードの登録・暗号化にのみ対応しています。パスワードの変更や類推性他の要素は運用でカバーして下さい。
6	マニュアルに従ってテキストエディタ等を利用して確認する必要があります。
7	オプションで時刻同期サービスを提供しています(別途ネット回線が必要)。施設の NTP サーバと同期することも可能です。
8	オプションでマルウェア対策ソフトウェアの導入が可能です。パターンファイルの定期更新は動作検証の関係から月 1 回となります。必要に応じて臨時の更新を行う場合があります。
9	サーバクライアント間で無線 LAN を導入する事が可能ですがアクセスポイントのセキュリティ設定に関して弊社では指定していませんのでお客様の方でガイドラインに合わせて導入お願いします。弊社で推奨のアクセスポイントを設定する場合はガイドラインに沿った設定を行います。
10	施設様の方でソフトウェアのインストールは絶対に行わないで下さい。
11	外部入出力に関して施設様の運用で対応していただく必要があります。
12	運用開始時に予め非常用アカウントの作成をお願いします。
13	オプションの保守サービスに入る必要があります。詳細は弊社担当者にお問い合わせ下さい。
14	ネットワーク機器側の設定をお願いします。
15	電子署名をご使用の際は別途、他社製ソフトウェアの導入が必要となります。
16	NTP による時刻同期機能を持っています。
17	ログから確認は行えますが機能としては準備されていません。
18	オプションのネットワーク保管サービスを申し込むことにより、データセンターに保管されている画像データを参照することが可能です。画像診断には適切な読影装置(医療用モニタ)を使用する必要があります。
19	監査証跡のフォーマットは公開しておりますので、ログサーバにて解析してください。
20	バックアップには DVD-R、NAS、データセンターなど複数の対象をオプションで用意していますので弊社担当者にご相談下さい。
21	DICOM 形式での出力が可能です。
22	オプションで複合機を使用したドキュメントの取り込み機能を提供しています。
23	安全管理ガイドラインの基準に適合した複合機をご使用ください。

- 想定するシナリオ

①製造事業者が自社の製品のセキュリティ関連機能についてMDSを作成

②医療機関からの要求により製造事業者が提出、あるいは、製造業者が自身のホームページで公開

③医療機関は受け取った開示説明書を元にリスクアセスメントを行い、適切な運用が行われるように対応



統一された書式のMDSは、医療機関での効率的なリスクアセスメントの実施に有効なツールとして活用できる。

MDS-WG

- 16年度活動概要
  - “「製造業者による医療情報セキュリティ開示書」ガイドに関するQ&A”の作成及びHP公開
    - ✓15年度セミナーアンケートのフィードバック等
  - JSRT秋季学術大会・JIRAワークショップでの発表
    - ✓施設担当者への紹介
  - Ver.3.0改訂作業
    - ✓今まで出された質問や問題点の反映
    - ✓質問数に変更が起きたためVer.2.1の予定から変更
  - 第2回・書き方セミナーの開催(2/24予定)
    - ✓安全管理GL第4.4版対応
    - ✓電子カルテシステムを題材(第1回はPACS)

MDS-WG

- 17年度活動予定
  - 安全管理GL第4.4版、第5版に対する改訂作業
  - ITEM2017での冊子配布
  - 書き方セミナーの開催(JIRA向け企画の検討)
  - 他、普及活動の検討

「6.2 医療機関等における情報セキュリティマネジメントシステム（ISMS）の実践」B項において、MDSのチェックリストが情報のリストアップ、リスク分析・対策に役立つ旨が紹介されており、今後、医療機関からメーカーへの要求が増えると予想され、普及活動が重要となる。

サイバーセキュリティ

- 厚生労働省通知「医療機器におけるサイバーセキュリティの確保について」(2015年4月発出)
  - 医療機器製造販売業者に対して、リスクマネジメントにより、医療機器へのサイバーリスクの適切な対応を要求
  - 具体的な対応として以下を要求

① 他の機器・ネットワーク等と接続して使用する又は他からの不正なアクセス等が想定される医療機器については、当該医療機器で想定されるネットワーク使用環境等を踏まえてサイバーリスクを含む危険性を評価・除去し、防護するリスクマネジメントを行い、使用者に対する必要な情報提供や注意喚起を含めて適切な対策を行うこと。

② ①の必要なサイバーセキュリティの確保がなされていない医療機器については、使用者に対してその旨を明示し、他との接続を行わない又は接続できない設定とするよう必要な注意喚起を行うこと。

③「医療情報システムの安全管理に関するガイドライン」を踏まえ、医療機関における不正ソフトウェア対策やネットワーク上からの不正アクセス対策等のサイバーセキュリティの確保が適切に実施されるよう、医療機関に対し、必要な情報提供を行うとともに、**必要な連携**を図ること。

サイバーセキュリティ

- 3J(JAHIS,JEITA,JIRA)で通知内容を具体化し、ガイダンスのドラフトを作成、医機連を通してAMED研究班の成果物として厚労省から出される予定。
  - ✓パブリックコメントが出されるのを待っている状態

- FDA：医療機器のサイバーセキュリティの市販後管理(Postmarket Management of Cybersecurity in Medical Devices)
  - ✓16年12月に正式版が公開された。
  - ✓JIRAから翻訳が公開されている。(会員検討用途)

サイバーセキュリティ

- 広報活動
  - 第72回日本放射線技術学会総会学術大会
    - 医療機器におけるサイバーセキュリティの確保に関して(16年4月)
  - 第44回日本放射線技術学会秋季学術大会
    - JIRAワークショップ　医療機器に対するサイバーセキュリティへの対応(16年10月)

IoTセキュリティガイダンス

- 背景

  IoTでは、これまで接続されていなかった自動車やカメラなどの機器が、WiFiや携帯電話網などを介してインターネットに接続されることにより、新たな脅威が発生し、それに対するセキュリティ対策が必要となった。

  – IoT推進コンソーシアム(総務省、経済産業省)から、16年7月に公表された。

IoTセキュリティガイダンス

■IoT機器やシステム、サービスの提供にあたってのライフサイクル（方針、分析、設計、構築・接続、運用・保守）における指針を定めるとともに、一般利用者のためのルールを定めたもの。
■各指針等においては、具体的な対策を要点としてまとめている。

	指針	主な要点
方針	IoTの性質を考慮した基本方針を定める	● 経営者がIoTセキュリティにコミットする。 ● 内部不正やミスに備える。
分析	リスクを認識する	● 守るべきものを特定する。 ● つながることによるリスクを想定する。
設計	守るべきものを守る設計を考える	● つながる相手に迷惑をかけない設計をする。 ● 不特定の相手とつなげられても安全安心を確保できる設計をする。 ● 安全安心を実現する設計の評価・検証を行う。
構築・接続	ネットワーク上での対策を考える	● 機能及び用途に応じて適切にネットワーク接続する。 ● 初期設定に留意する。 ● 認証機能を導入する。
運用・保守	安全安心な状態を維持し情報発信・共有を行う	● 出荷・リリース後も安全安心な状態を維持する。 ● 出荷・リリース後もIoTリスクを把握し、関係者に守ってもらいたいことを伝える。 ● IoTシステム・サービスにおける関係者の役割を認識する。 ● 脆弱な機器を把握し、適切に注意喚起を行う。
一般利用者のためのルール		● 問合せ窓口やサポートがない機器やサービスの購入・利用を控える。 ● 初期設定に気をつける。 ● 使用しなくなった機器については電源を切る。

まとめ

- TC215 WG4については規格検討に継続的に取り組むとともにISO/TS11633の改定活動に注力する。また、セキュリティに関連する他WGやDICOM等の規格に対しても積極的に関与する。
- 安全管理GLについては個人情報保護法も含め、改定作業に引き続き関与し、MDSの継続的な更新作業、セミナー等の普及活動等を継続する。
- サイバーセキュリティ、IoT、ビッグデータの活用等、セキュリティに対する要求が国内外で益々深まっており、タイミング良く適切な対応を行っていく。

御清聴 ありがとうございました。